

UNITED STATES DISTRICT COURT

FILED
ASHEVILLE, NC

for the

Western District of North Carolina

JUL 16 2019

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*

1730 Nolan Wood Hts, Morganton, North Carolina,
 28655, all vehicles, outbuildings and appurtenances

Case No.

1:19 mj 61

U.S. DISTRICT COURT
W. DISTRICT OF N.C.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
 See Attachment A

located in the Western District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:
 See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252(a)(1)	Transportation of Child Pornography
18 U.S.C. § 2252(a)(2)	Distribution/Receipt of Child Pornography
18 U.S.C. § 2252(a)(4)	Possession of Child Pornography

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's Signature

Jacob R Guffey, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

7/16/2019


 Judge's signature

City and state: Asheville, North Carolina

W. Carleton Metcalf, U.S. Magistrate Judge

Printed name and title

FILED
ASHEVILLE, NC

JUL 16 2019

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

U.S. DISTRICT COURT
W. DISTRICT OF N.C.

IN THE MATTER OF THE SEARCH OF:

THE RESIDENCE LOCATED AT
1730 NOLAN WOOD HTS
MORGANTON, NORTH CAROLINA
28655

Case No. 1:19mj 41

ATTACHMENT C:
AFFIDAVIT OF JACOB R GUFFEY
IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jacob R GUFFEY, being duly sworn, depose and state as follows:

1. I am a Special Agent of the FBI, assigned to the Charlotte Division, Hickory Resident Agency, Hickory, North Carolina, and I am the case agent for this investigation.
2. I have been a Special Agent since 2008 and I am currently assigned to the Charlotte Division, Hickory Resident Agency. In this capacity, I am assigned to investigate cases involving Child Pornography, corporate fraud, public corruption, and similar violations. From 2012 to 2015, I worked on the Navajo Indian Reservation, located within the Area of Responsibility of the Albuquerque Division, Gallup Resident Agency. At that assignment I conducted and participated in numerous death investigations, child sexual assaults, and other federal crimes occurring within the boundaries of Indian Country. From 2008 to 2012 I investigated Health Care Fraud in

the Miami Division. I have personally been the case agent for numerous investigations that have resulted in the indictment and conviction of numerous subjects. I have also participated in ordinary methods of investigation, including but not limited to, consensual monitoring, physical surveillance, interviews of witnesses and subjects, and the use of confidential informants. I am an active member of the Evidence Response Team. Accordingly, I have executed numerous search warrants and seized evidence. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am investigating the activities of the internet account registered to Rhonda Bivens. Also living at the residence is Wayne Hudson. That residence is 1730 Nolan Wood Hts, Morganton, North Carolina, 28655. As will be shown below, there is probable cause to believe that someone using the internet account registered to Rhonda Bivens at 1730 Nolan Wood Hts, Morganton, North Carolina, 28655 has transported, received, possessed, and distributed child pornography, in violation of 18 U.S.C. §§ 2252(a)(1), (a)(2) and (a)(4). I submit this Application and Affidavit in support of a search warrant authorizing a search of the property and residence at 1730 Nolan Wood Hts, Morganton, North Carolina, 28655 as further described in Attachment A. Located within the premises to be searched, I seek to seize evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing transportation, receipt, possession and distribution of child pornography. I request authority to search the entire premises, including the residential dwelling, vehicles located on the property, or any outbuildings such as detached garage, sheds or barns.

In addition, I request authority to search any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

4. The statements in this Affidavit are based in part on information provided by FBI undercover employees and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of 18 U.S.C. § 2252 are presently located at 1730 Nolan Wood Hts, Morganton, North Carolina, 28655.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. § 2252 relating to material involving the sexual exploitation of minors.
 - a. 18 U.S.C. § 2252(a)(1) makes it a crime to knowingly transport or ship, using any means or facility of interstate commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction was of such conduct.

- b. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction was of such conduct.
- c. 18 U.S.C. § 2252(a)(4) prohibits possessing or accessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that have traveled in interstate or foreign commerce.

DEFINITIONS

- 6. The following definitions apply to this Affidavit and Attachment B:
 - a. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of

themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

- b. “Child Pornography” includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).
- c. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” *See* 18 U.S.C. § 1030(e)(1).
- d. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices);

peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- e. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- f. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- g. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works.

Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- h. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. Like a phone number, no two computers or network of computers connected to the internet are assigned the same IP address at exactly the same date and time. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.
- i. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).
- j. “Peer-to-peer file-sharing” “P2P” is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user’s computer, conducting searches for files that are

currently being shared on another user's computer and then downloading files from the other user's computer.

- k. "Sexually explicit conduct" refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).
- l. "Shared Folder" is a folder of files stored on a computer's local hard disk drive that can be used (or shared) by other users on the network or internet.
- m. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).
- n. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices

such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.
8. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
9. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.
11. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.
12. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.
13. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained

unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

14. A growing phenomenon on the Internet is peer-to-peer file-sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the Internet. There are multiple types of P2P file sharing networks on the Internet. To connect to a particular P2P file sharing network, a user first obtains a P2P client software program for a particular P2P file sharing network, which can be downloaded from the Internet. A particular P2P file sharing network may have different P2P client software programs that access to that particular P2P file sharing network. Additionally, a particular P2P client software program may be able to access multiple P2P file sharing networks. These P2P client software programs share common protocols for network access and file sharing. The user interface, features, and configurations may vary between clients and versions of the same client.

15. In general, P2P client software allows the user to set up file(s) on a computer to be shared on a P2P file sharing network with other users running compatible P2P client software. A user can also obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network.
16. Some P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files that they are not sharing. Typically, settings within these programs control sharing thresholds.
17. Typically, during a default installation of a P2P client software program, settings are established which configure the host computer to share files. Depending upon the P2P client software used, a user may have the ability to reconfigure some of those settings during the installation or after the installation has been completed.
18. Typically, a setting establishes the location of one or more directories or folders whose contents (digital files) are made available for distribution to other P2P clients. In some clients, individual files can also be shared.
19. Typically, a setting controls whether or not files are made available for distribution to other P2P clients.

20. Typically, a setting controls whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.
21. Typically, files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value is computed for each file and/or piece of a file being shared (dependent on the P2P file sharing network), which uniquely identifies it on the network. A file (or piece of a file) processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their names. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, typically, users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from the exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.
22. P2P file sharing networks, including the BitTorrent network, are frequently used to trade digital files of child pornography. These files include both image and movie files.

23. The BitTorrent network is a very popular and publically available peer to peer file sharing network. Most computers that are part of this network are referred to as "peers." The terms "peers" and "clients" can be used interchangeably when referring to the BitTorrent network. A peer can simultaneously provide files to some peers while downloading files from other peers.
24. The BitTorrent network can be accessed by computers running many different client programs, some of which include the BitTorrent client program, µTorrent client program and Vuze client program. These client programs are publically available and free P2P client software programs that can be downloaded from the Internet. There are also BitTorrent client programs that are not free. These BitTorrent client programs share common protocols for network access and file sharing. The user interface, features, and configuration may vary between clients and versions of the same client.
25. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files. Depending upon the BitTorrent client used, a user may have the ability to reconfigure some of those setting during installation or after the installation has been completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to other BitTorrent network users to download.
26. In order to share a file or a set of files on the BitTorrent network, a "Torrent" file needs to be created by the user that initially wants to share the file or set of files. A "Torrent" is typically a small file that describes the file(s) that are being shared, which may

include information on how to locate the file(s) on the BitTorrent network. A typical BitTorrent client will have the ability to create a "Torrent" file. It is important to note that the "Torrent" file does not contain the actual file(s) being shared, but information about the file(s) described in the "Torrent," such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent". The "info hash" is a SHA-1 hash value of the set of data describing the file(s) referenced in the Torrent, which include the SHA-1 hash value of each file piece, the file size, and the file name(s). The info hash of each Torrent uniquely identifies the Torrent file on the BitTorrent network. The Torrent file may also contain information on how to locate file(s) referenced in the Torrent by identifying "Trackers." Trackers are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the Torrent file. A Tracker is only a pointer to peers/clients on the network who may be sharing part or all of the files referenced in the Torrent. It is important to note that the Trackers do not actually have the file(s) and are used to facilitate the finding of other peer/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of Tracker(s) on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular Torrent file. There are many publically available servers on the Internet that provide BitTorrent tracker services.

27. Once a Torrent is created, in order to share the file(s) referenced in the Torrent file, a user typically makes the Torrent available to other users, such as via websites on the Internet.
28. In order to locate Torrent files of interest, a typical user will use keyword searches within the BitTorrent network client itself or on the websites hosting Torrents. Once a Torrent file is located that meets the keyword search criteria, the user will download the Torrent file to their computer. Alternatively, a user can also search for and locate "magnet links", which is a link that enables the BitTorrent network client program itself to download the Torrent file to the computer. In either case, a Torrent file is downloaded to the user's computer. The BitTorrent network client will then process the Torrent file in order to find Trackers or utilize other means that will help facilitate finding other peer/clients on the network that have all or part of the file(s) referenced in the Torrent file. It is again important to note that the actual file(s) referenced in the Torrent are actually obtained directly from other peers/clients on the BitTorrent network and not the Trackers themselves. Typically, the Trackers on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on the SHA-1 info hash comparison), or parts of the same file(s), referenced in the Torrent, to include the remote peers/clients Internet Protocol (IP) addresses.
29. For example, a person interested in obtaining child pornography images on the BitTorrent network would open the BitTorrent client application on his/her computer

and conduct a keyword search for files using a term such as "preteen sex." The results of the Torrent search are typically returned to the user's computer by displaying them on the Torrent hosting website. The hosting website will typically display information about the Torrent, which can include the name of the Torrent file, the name of the file(s) referenced in the Torrent file, the file(s), and the "info hash" SHA-1 value of the Torrent file. The user then selects a Torrent of interest to download to their computer. Typically, the BitTorrent client program will then process the Torrent file. The user selects from the results displayed, the file(s) they want to download that were referenced in the Torrent file. Utilizing trackers and other BitTorrent network protocols (such as Distributed Hash Tables, Peer Exchange and Local Peer Discovery), peers/clients are located that have reported they have the file(s) or parts of the file(s) referenced in the torrent file available for sharing. The file(s) is then downloaded directly from the computer(s) sharing the file. Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 piece hash described in the torrent file. During the download process, a typical BitTorrent client program displays the Internet Protocol address of the peers/clients that appear to be sharing part or all of the file(s) referenced in the Torrent file or other methods utilized by the BitTorrent network protocols. The downloaded file is then stored in the area previously designated by the user and/or client program. The downloaded file(s), including the Torrent file, will remain until moved or deleted.

30. Typically, as described above, one method for an investigator to search the BitTorrent network for users possessing and/or disseminating child pornography files is to type in search terms, based on training and experience, that would return a Torrent file indicative of child pornography. The investigator would then download the file(s) referenced within the Torrent file and determine if the file(s) indeed contained child pornography. If so, the investigator can document the info hash SHA-1 hash value of this torrent file, to be compared with future identical Torrent files observed on the BitTorrent network. Although transparent to the typical user, when searches are conducted, additional results are received from the trackers on other peers who recently reported to the network as having file(s) in whole or in part, which may include the IP addresses of those peers/clients. This information can be documented by investigators and compared to those info hash SHA-1 hash values the investigator has obtained in the past and believes to be child pornography. This allows for the detection and investigation of computers involved in possessing, receiving, and/or distributing files of previously identified child pornography. Therefore, without even downloading the file, the investigator can compare the info hash SHA-1 hash value and determine with mathematical certainty that a file(s) seen on the network is an identical copy of a child pornography file(s) they have seen before.

31. The returned list of IP addresses can include computers that are likely to be within the investigator's jurisdiction. The ability to identify the approximate location of these IP addresses is provided by geographic mapping services, which are publicly available and also used for marketing and fraud detection. At this point in the investigative

process, an association between a known Torrent file (based upon the info hash value comparison) and a computer having a specific IP address (likely to be located within a specific region) can be established.

32. Once a client user is identified as recently having a file(s) believed to be child pornography, in whole or in part, the investigator can then query the client user directly to confirm the client user has that file(s), in whole or in part, and/or download that file directly from the client user exclusively, otherwise known as a single source download. Depending upon several factors, including configuration and available resources, it might not be possible to do either. The process of sharing files on BitTorrent network involves peers allowing other peers to copy a file(s) or portions of a file(s). This sharing process does not remove the file(s) from the computer sharing the file. This process places a copy of the file on the computer which downloaded it.
33. If an investigator either received an affirmative response from a remote peer that they possess a digital file, or the investigator received a digital file, in whole or in part, that is believed to contain child pornography, from a remote peer at a specific IP address, the investigator can conclude that a computer, likely to be in this jurisdiction, is running a BitTorrent P2P client and is currently possessing, receiving, and/or distributing specific and known depictions of child pornography.
34. Law enforcement has created BitTorrent network client programs that obtain information from Trackers about peers/clients recently reporting that they are involved in sharing digital files of known actual child pornography (based on the info hash SHA-

1 hash value), which then allows the downloading of a file from a single IP address (as opposed to obtaining the file from multiple peers/clients on the network). This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography on the BitTorrent network.

35. During the query and/or downloading process from a remote BitTorrent network client, certain information may be exchanged between the investigator's client and the remote client they are querying and/or downloading from, such as 1) the remote client's IP address; 2) a confirmation from the remote client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the remote client program; and 3) the remote client program and version. This information may remain on the remote client's computer system for long periods of time. The investigator has the ability to log this information. A search can later be conducted on a seized computer system(s) for this information, which may provide further evidence that the investigator's client communicated with the remote client.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

36. Based on my knowledge, training, and experience, I know that computer storage devices, such as a computer hard drive, can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensics tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes

be recovered with forensics tools. Forensic tools can retrieve files and data that the user has attempted to delete or that have been overwritten by the file system. Even files that were deleted months or years ago can often be retrieved by computer forensic software.

37. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:
38. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
39. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize

in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, deleted, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

40. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).
41. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

PROBABLE CAUSE

42. On March 27, 2019, an online undercover employee of the FBI used a BitTorrent application to conduct undercover investigations into the sharing of child pornography.

During this investigation, a computer sharing child pornography was located on the BitTorrent file sharing network.

43. On March 27, 2019, the undercover employee located a computer with the IP address 75.143.178.147 on the BitTorrent file sharing network sharing files that have been previously identified as files of interest in these child pornographic investigations.
44. On March 27, 2019, the undercover employee downloaded files of interest directly from IP Address 75.143.178.147. Approximately 24 of those files were videos containing child pornography. The following are descriptions of some of those files:
 - a. Video titled, “!!!NEW!!! 2010 Kait 5yo – chunk2FK pthc best.avi” found in a folder labeled, “preteen HQ”. The video was approximately 3 seconds long and depicted a female who appeared to be under the age of 3, who was naked. An adult male was engaging in vaginal sex with the female.
 - b. Video titled, “lsd04-08-01.avi” found in a folder labeled, “Ls – Dreams 04 (Pandora’s Box)”. The video was approximately 3:38 in length. The video depicted a female who appeared to be under the age of 18 and over the age of 12. The female was wearing a green night gown, which she removes and is then completely nude. The video is a close up of her breasts and vagina.
 - c. Video titled, “lsd04-03-02.avi” found in a folder labeled, “Ls – Dreams 04 (Pandora’s Box)”. The video was approximately 5:51 in length. The video depicts a female who appears to be under the age of 18 and over the age of 12

wearing a red skirt and not shirt or underwear. She is on her hands and knees with the video camera recording closely to her exposed vagina.

- d. Video titled, "lsd04-09-02.avi" found in a folder labeled, "Ls – Dreams 04 (Pandora's Box)". The video was approximately 5:05 in length. The video depicts a female who appears to be under the age of 18 and over the age of 12. She is completely nude. The focal point of the video is of her exposed breasts and vagina.
- e. Video titled, "(Hussyfan)(pthc)(r@gold)(babyshivid)-K-KI!!NEW – WetB4ass(marissa).avi" found in a folder labeled, "ptsc". The video was approximately XXX in length and depicts 2 nude females who appear under the age of 18 and over the age of 12. They are laying on a bed and rubbing each other's vaginas.

- 45. On March 27, 2019, a Special Agent of the FBI queried IP address 75.143.178.147 through arin.net which showed it was registered with Charter Communications, Inc.
- 46. On March 28, 2019, an Administrative Subpoena was served to Charter Communications requesting subscriber related information for the account assigned IP address 75.143.178.147.
- 47. On March 29, the Special Agent received the following information from Charter Communications, Inc in response to the aforementioned Administrative Subpoena:

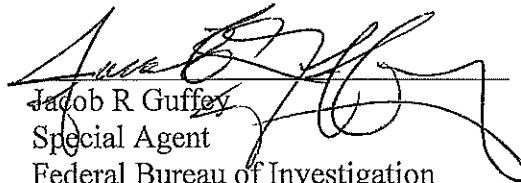
a.	Full Name:	Rhonda Bivens
b.	Account Number:	8351400280212788
c.	Address:	1730 Nolan Wood Hts, Morganton, NC 28655-7716
d.	MAC:	f4:8e:38::8e:4b:88
e.	Phone number:	828-433-7156
f.	Email address:	<u>wormy73@charter.net</u>
g.	Email address:	<u>rkbivens@charter.net</u>
h.	Current Lease Start Date:	March 20, 2019 1:36:57 PM
i.	Lease End Date:	March 27, 2019 7:14:26 PM

48. On May 30, 2019, your Affiant conducted physical surveillance of 1730 Nolan Wood Hts, Morganton, NC, 28655. Your Affiant observed 2 vehicles parked out front. The area where a license plate should be was not visible. Your Affiant observed the street number posted on the house next to the front door.
49. On July 2, 2019, your Affiant conducted a search of the Burke County Global Information System (GIS) and found that 1730 Noland Wood Hts, Morganton, NC, 28655 was owned by Rhonda K Bivens.
50. On July 2, 2019, your Affiant searched NC driver's license information and discovered that Wayne Allen Hudson listed 1730 Nolan Wood Hts, Morganton, NC, 28655 as his residence.
51. On July 2, 2019, your Affiant conducted physical surveillance of 1730 Nolan Wood Hts, Morganton, NC, 28655. During the surveillance your Affiant knocked at the front door. A man opened the door and identified himself as Wayne Hudson. Your Affiant asked if the 2 cars in the front were for sale. He advised that he owned a mechanic shop called Wormy's, and the 2 cars were not his. Wayne Hudson did not ask your Affiant


his name, nor did your Affiant provide it. During your Affiant's conversation Wayne Hudson stated he had lived at that address for approximately 40 years. He stated the county brought water and power to his road and he used "Charter Spectrum" for his internet.

CONCLUSION

52. Based on the aforementioned factual information, your Affiant respectfully submits that there is probable cause to believe that an individual at the residence described above is involved in transportation, receipt, possession and distribution of child pornography. Your Affiant respectfully submits that there is probable cause to believe that an individual the residence described above has violated 18 U.S.C. §§ 2252. Additionally, there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2252(a)(1), (a)(2) and (a)(4), is located in the residence described in Attachment A, and this evidence, listed in Attachment B to this Affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.
53. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.


Jacob R. Guffey
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 16th day of July, 2019.


W. CARLETON METCALF
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF NORTH CAROLINA

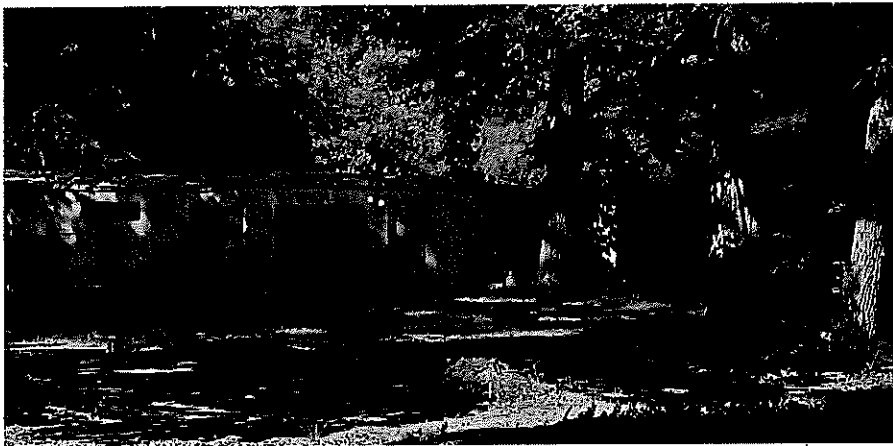
Attachment A
Place to be Searched

The residence, outbuildings, structures, appurtenances, and vehicles located at 1730 Nolan Wood Hts, Morganton, North Carolina, 28655. The residence is described as a single story single wide trailer with light siding, and dark shutters. The house number is posted on the right side of the front door. The search location includes any structures, outbuildings, appurtenances, and vehicles located at 1730 Nolan Wood Hts, Morganton, North Carolina, 28655.

Buildings to be searched:

1730 Nolan Wood Hts, Morganton, North Carolina, 28655

The residence is described as a single story single wide trailer with light siding, and dark shutters.



ATTACHMENT B

Information to be Seized

1. Instrumentalities of the violations contained within the application for the search warrant at 1730 Nolan Wood Hts, Morganton, North Carolina, 28655:

a. any computer, computer system, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, hard drive and other computer related operation equipment, photographs and other visual depictions of such graphic interchange formats (JPG, GIF, TIF, AVI, and MPEG), electronic data storage devices (hardware, software, diskettes, backup tapes, CDs, DVD, flash memory devices, thumb drives, and other storage media); and any input/output peripheral devices, passwords, data security devices, and related security documentation;

b. books and magazines containing visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A);

c. originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A); and

d. motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A).

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

k. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet;

4. Any child pornography as defined by 18 U.S.C. § 2256(8);

5. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence;

6. Documents and records regarding the ownership and/or possession of the searched premises;

7. Credit card information, bills, and payment records;

8. Information or correspondence pertaining to affiliation with any child exploitation websites;

9. Any material that is “child erotica”;

10. Any correspondence/records indicating the true identity of any member or user of “BitTorrent” and;

11. Any correspondence, e-mails, electronic messages, and records pertaining to “BitTorrent”

As used above, the terms “records” and “information” refer to all forms of creation or storage, any form of computer or electronic storage (such as hard disks or other media that can

store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, videotapes, motion pictures, or photocopies).

The term "computer" refers to all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions: desktop computers, notebook computers, mobile phones, tablets, server computers, smart phones, and network hardware.

The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples are hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.